Vector Invariants of a Class of Pseudoreflection Groups and Multisymmetric Syzygies

M. Domokos[*]

Communicated by F. Knop

Abstract.   First and second fundamental theorems are given for polynomial invariants of a class of pseudo-reflection groups (including the Weyl groups of type B_n), under the assumption that the order of the group is invertible in the base field. As a special case, a finite presentation of the algebra of multisymmetric polynomials is obtained. Reducedness of the invariant commuting scheme is proved as a by-product. The algebra of multisymmetric polynomials over an arbitrary base ring is revisited.
Mathematics Subject Classification 2000: 13A50, 14L30, 20G05.
Key Words and Phrases: Multisymmetric polynomials, reflection groups, polynomial invariant, second fundamental theorem, ideal of relations, trace identities.

1.   Introduction

Fix natural numbers n and q, and a field K. Apart from Theorem 2.7 and Section 5, we shall assume that $n!q$ is invertible in K, and assume that K contains a primitive qth root of 1. Denote by $G = G(n,q)$ the subgroup of $GL(n,K)$ consisting of the monomial matrices whose non-zero entries are qth roots of 1. The order of G is $n!q^n$, and as an abstract group, G is isomorphic to the wreath product of the cyclic group C_q of order q and the symmetric group S_n; that is, G is isomorphic to a semi-direct product $(C_q \times \cdots \times C_q) \rtimes S_n$.

Consider the natural action of G on $V = K^n$. Since G is generated by pseudo-reflections, by the Shephard-Todd Theorem [37] (see [7] for a uniform proof in characteristic zero, and [39] for the case when $\mathrm{char}(K)$ is positive and co-prime to the order of G) the algebra $K[V]^G$ of polynomial invariants is generated by algebraically independent elements. Now consider the diagonal action of G on $V^m = V \oplus \cdots \oplus V$, the direct sum of m copies of V. The algebra $K[V^m]^G$ is no longer a polynomial ring if $m \geq 2$ (and G is not the trivial group). In the present paper we show a very short and simple argument that yields simultaneously the generators of $K[V^m]^G$ (first fundamental theorem) and the relations among these

generators (second fundamental theorem). Our main result is Theorem 3.2, which provides an explicit finite presentation of $K[V^m]^{G(n,q)}$ in terms of generators and relations. In the proof we apply Derksen's degree bound on syzygies [9] and ideas of Wallach and Garsia [20].

In the special case $q = 1$ we have $G = S_n$, and $K[V^m]^{S_n}$ is the algebra of multisymmetric functions, which received much attention in the literature (see the references in Remark 2.6 (ii)). Our approach gives new insight even in this special case, especially by its simplicity and transparency. We mention also that no finite presentation of the algebra of multisymmetric functions appeared in prior work (apart from the case of $\mathrm{char}(K) = 2$ studied in [15]).

Another interesting special case is when $q = 2$, and the group G is the Weyl group of type B_n. The generators of $K[V^m]^{G(n,2)}$ were determined in [23] and [22]. To the best of our knowledge, the second fundamental theorem has never been considered in the literature when $q > 1$.

The fundamental relation appearing here can be deduced from the theory of trace identities of matrices. This observation leads to the corollary that the $GL(n, \mathbb{C})$-invariant commuting scheme is reduced, see Theorem 4.1.

The present paper joins the content of our preprints [12] and [13] (some digressions from the preprints have been omitted). In addition, in Section 5 we adjust our method for arbitrary base rings and clarify and strengthen the known results in this case. In particular, in Theorem 5.5 we give a new characteristic free (infinite) presentation of the ring of multisymmetric polynomials.

2.   An infinite presentation

Denote by $x(i)_j$ the function on V^m mapping an m-tuple of vectors to the jth coordinate of the ith vector component. The coordinate ring $K[V^m]$ is the mn-variable polynomial ring over K with generators $x(i)_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$.

There is a natural multigrading on $K[V^m]$ preserved by the action of G. Namely, $f \in K[V^m]$ has multidegree $\alpha = (\alpha_1, \ldots, \alpha_m)$, if it has degree α_i in the set of variables $x(i)_1, \ldots, x(i)_n$, for all $i = 1, \ldots, m$. Write $K[V^m]_\alpha^G$ for the multihomogeneous component of $K[V^m]^G$ with multidegree α. Consider the symbols $x(1), \ldots, x(m)$ as commuting variables, and denote by $\mathcal{M}(q)$ the set of non-empty monomials in the variables $x(i)$ whose degree is divisible by q. In particular, $\mathcal{M}(1)$ is the set of all non-empty monomials in the variables $x(i)$. For $w = x(1)^{\alpha_1} \cdots x(m)^{\alpha_m} \in \mathcal{M}(q)$ set $w_{\langle j \rangle} = x(1)_j^{\alpha_1} \cdots x(m)_j^{\alpha_m}$, and define

$$[w] = \sum_{j=1}^n w_{\langle j \rangle}.$$

(These are *polarizations* of the usual *power sum symmetric functions*.) Note that the multidegree of $[w]$ is α. Since for all $j = 1, \ldots, n$ and $w \in \mathcal{M}(q)$, the term $w_{\langle j \rangle}$ is invariant with respect to the normal subgroup N consisting of the diagonal matrices in G, the S_n-invariant polynomial $[w]$ is G-invariant. Sometimes we shall think of the $x(i)$ as the generic diagonal matrices $\mathrm{diag}(x(i)_1, \ldots, x(i)_n)$, $i = 1, \ldots, m$, and then $[w]$ is nothing but the trace of the diagonal matrix w.

Proposition 2.1.   *The products $[w_1] \cdots [w_r]$ with $r \leq n$, $w_i \in \mathcal{M}(q)$ constitute a K-vector space basis of $K[V^m]^{G(n,q)}$.*

Proof.   An arbitrary monomial $u \in K[V^m]$ in the variables $x(i)_j$ can be written as $u = u_{\langle 1 \rangle}^1 \cdots u_{\langle n \rangle}^n$ with a unique n-tuple $(u^1, \ldots, u^n)$ of monomials in $\mathcal{M}(1) \cup \{1\}$. The algebra $K[V^m]^N$ is spanned by the u with $u^1, \ldots, u^n \in \mathcal{M}(q) \cup \{1\}$. The action of S_n permutes these monomials, and since $G(n,q)$ is generated by N and S_n, the S_n-orbit sums of the N-invariant monomials of multidegree α form a basis in $K[V^m]_\alpha^G$. For a multiset $\{w_1, \ldots, w_r\}$ with $r \leq n$, $w_i \in \mathcal{M}(q)$, denote by $O_{\{w_1,\ldots,w_r\}}$ the S_n-orbit sum of the monomial $w_{1\langle 1 \rangle} \cdots w_{r \langle r \rangle}$. Call r the *height* of this *monomial multisymmetric function*. Set $T_{\{w_1,\ldots,w_r\}} = [w_1] \cdots [w_r]$.

So the $O_{\{w_1,\ldots,w_r\}}$ with $\mathrm{multideg}(w_1 \cdots w_r) = \alpha$ form a basis in $K[V^m]_\alpha^G$. Assume that the multiset $\{w_1, \ldots, w_r\}$ contains d distinct elements with multiplicities $r_1, \ldots, r_d$ (so $r_1 + \cdots + r_d = r$), then expanding $T_{\{w_1,\ldots,w_r\}}$ as a linear combination of monomial multisymmetric functions, the coefficient of $O_{\{w_1,\ldots,w_r\}}$ is $r_1! \cdots r_d!$ (which is non-zero by our assumption on the characteristic of K), and all other monomial multisymmetric functions contributing have height strictly less than r. This clearly shows the claim.   ∎

Remark 2.2.   After writing [12] we noticed that the special case $q = 1$ of Proposition 2.1 appears as Corollary 2.3 of [3] (see also Section 3 of [4] for the interpretation needed here).

Associate with $w \in \mathcal{M}(q)$ a variable $t(w)$, and consider the polynomial ring
$$\mathcal{F}(q) = K[t(w) \mid w \in \mathcal{M}(q)]$$
in infinitely many variables. Denote by
$$\varphi(q) : \mathcal{F}(q) \rightarrow K[V^m]^{G(n,q)}$$
the K-algebra homomorphism induced by the map $t(w) \mapsto [w]$. This is a surjection by Proposition 2.1. Next we introduce a uniform set of elements in its kernel. For a multiset $\{w_1, \ldots, w_{n+1}\}$ of $n+1$ monomials from $\mathcal{M}(q)$, we associate an element $\Psi(w_1 \ldots, w_{n+1}) \in \mathcal{F}(q)$ as follows. Write $\mathcal{P}_{n+1}$ for the set of partitions $\lambda = \lambda_1 \cup \cdots \cup \lambda_h$ of the set $\{1, \ldots, n+1\}$ into the disjoint union of non-empty subsets λ_i, and denote $h(\lambda) = h$ the number of parts of the partition λ. Set

$$\Psi(w_1, \ldots, w_{n+1}) = \sum_{\lambda \in \mathcal{P}_{n+1}} (-1)^{h(\lambda)} \prod_{i=1}^{h(\lambda)} \left((|\lambda_i| - 1)! \cdot t(\prod_{s \in \lambda_i} w_s) \right).$$

(See Section 6 for examples.)

Proposition 2.3.   *The kernel of $\varphi(q)$ contains the element $\Psi(w_1, \ldots, w_{n+1})$ for arbitrary $w_1, \ldots, w_{n+1} \in \mathcal{M}(q)$.*

Proof.   One way to see it is to specialize the fundamental trace identity of $n \times n$ matrices to diagonal matrices. Indeed, let $Y(1), \ldots, Y(n+1)$ be generic $n \times n$

matrices (so their entries generate an $(n+1)n^2$-variable commutative polynomial ring). For a permutation $\pi \in S_{n+1}$ with cycle decomposition

$$\pi = (i_1 \cdots i_d) \cdots (j_1 \ldots j_e)$$

set

$$\mathrm{Tr}^\pi = \mathrm{Tr}(Y(i_1) \cdots Y(i_d)) \cdots \mathrm{Tr}(Y(j_1) \cdots Y(j_e)).$$

Then we have the equality

$$\sum_{\pi \in S_{n+1}} \mathrm{sign}(\pi)\mathrm{Tr}^\pi = 0 \tag{1}$$

called the *fundamental trace identity* of $n \times n$ matrices. (This can be obtained by multilinearizing the Cayley-Hamilton identity to get an identity multilinear in the n matrix variables $Y(1), \ldots, Y(n)$, and then multiplying by $Y(n+1)$ and taking the trace; see for example [18] for details.) The substitution $Y(i) \mapsto w_i$ $(i = 1, \ldots, n+1)$ in (1) yields the result. ∎

Remark 2.4. We shall benefit in Section 4 from the fact that in the above proof we descend from a statement about non-commuting matrices. A more elementary proof is the following: express the $(n+1)$th elementary symmetric function in $n+1$ variables in terms of the first $n+1$ power sums using the Newton formulae; then multilinearize this identity, and specialize the $(n+1)$th coordinates to zero.

Theorem 2.5. (i) *The kernel of the K-algebra homomorphism $\varphi(q)$ is the ideal generated by the $\Psi(w_1, \ldots, w_{n+1})$, where $w_1, \ldots, w_{n+1} \in \mathcal{M}(q)$.*

(ii) *The algebra $K[V^m]^{G(n,q)}$ is minimally generated by the $[w]$, where $w \in \mathcal{M}(q)$ with $\deg(w) \leq nq$.*

Proof. (i) The coefficient in $\Psi(w_1, \ldots, w_{n+1})$ of the term $t(w_1) \cdots t(w_{n+1})$ is $(-1)^{n+1}$, and all other terms are products of at most n variables $t(u)$. So the relation $\varphi(q)(\Psi(w_1, \ldots, w_{n+1})) = 0$ can be used to rewrite $[w_1] \cdots [w_{n+1}]$ as a linear combination of products of at most n invariants of the form $[u]$ (where $u \in \mathcal{M}(q)$). So these relations are sufficient to rewrite an arbitrary product of the generators $[w]$ in terms of the basis given by Proposition 2.1. This obviously implies our statement about the kernel of $\varphi(q)$.

(ii) If $w \in \mathcal{M}(q)$ and $\deg(w) > qn$, then w can be factored as $w = w_1 \cdots w_{n+1}$ where $w_i \in \mathcal{M}(q)$. The term $t(w)$ appears in $\Psi(w_1, \ldots, w_{n+1})$ with coefficient $-(n!)$, which is invertible in K by our assumption on the characteristic. Therefore the relation $\varphi(q)(\Psi(w_1, \ldots, w_{n+1})) = 0$ shows that $[w]$ can be expressed as a polynomial of invariants of strictly smaller degree. It follows that $K[V^m]^{G(n,q)}$ is generated by the $[w]$, where $w \in \mathcal{M}(q)$ with $\deg(w) \leq nq$. This is a minimal generating system, because if $\deg(w) \leq nq$ for some $w \in \mathcal{M}(q)$, then $[w]$ can not be expressed by invariants of lower degree, since there is no relation among the generators whose degree is smaller than $(n+1)q$ by (i). ∎

Remark 2.6.   (i) In the special case $n = 1$ the above theorem gives the (classically known) defining relations of the q-fold Veronese embedding of the projective space $\mathbb{P}^{m-1}$ in $\mathbb{P}^d$, where $d = \begin{pmatrix} m + q - 1 \\ q \end{pmatrix} - 1$.

(ii) In the special case $q = 1$ our group is the symmetric group S_n and $K[V^m]^{S_n}$ is called the *algebra of multisymmetric polynomials*. It is an old result proved by Schläfli [36], MacMahon [28], Weyl [43], that when K has characteristic zero, this algebra is generated by the polarizations of the elementary symmetric polynomials (we mention that Noether [29] used this to prove her general degree bound on generating invariants of finite groups). The result on the generators was extended to the case $\mathrm{char}(K) > n$ by Richman [34] (see also [40], [5], [17] for other proofs). Counterexamples and further results on the generators in the case $0 < \mathrm{char}(K) \leq n$ are due to Fleischmann [16], Briand [5], Vaccarino [41]. The relations among the generators had been studied classically by Junker [24] [25], [26]. Working over $\mathbb{C}$ as a base field, an infinite presentation was given by Dalbec [8] (partly reformulating results of Junker [25]), and the special case $q = 1$ (and $K = \mathbb{C}$) of Theorem 2.5 appears in this explicit form in a recent paper by Bukhshtaber and Rees [6] (using a different language and motivation). Working over an arbitrary base ring K, [41] gives K-module generators of the ideal of relations among a reasonable infinite generating system (see Section 5).

(iii) In the special case $q = 2$ our group $G(n, 2)$ is the Weyl group of type B_n, and the ring of invariants $\mathbb{C}[V^m]^{G(n,2)}$ is isomorphic to the ring of invariants of the special orthogonal group $SO(2n + 1, \mathbb{C})$ acting via the adjoint representation on the commuting variety of its Lie algebra, and is also isomorphic to the ring of invariants of the symplectic group $Sp(2n, \mathbb{C})$ acting on the commuting variety of its Lie algebra (see for example [22] for this connection).

(iv) In our point of view, Theorem 2.5 (i) is a close relative of the result of Razmyslov [33] and Procesi [31] saying that all trace identities of $n \times n$ matrices are consequences of the fundamental trace identity. Their original approach is based on Schur-Weyl duality; Kemer in [27] gave an elementary combinatorial proof valid on the multilinear level in all characteristic.

(v) Identify V with the K-algebra of $n \times n$ diagonal matrices. Denote by $\mathrm{Mor}_{S_n}(V^m, V)$ the space of S_n-equivariant polynomial maps from V^m to V. Since S_n acts on V by algebra automorphisms, $\mathrm{Mor}_{S_n}(V^m, V)$ is a K-algebra with pointwise multiplication of maps $V^m \to V$. Identify the space $\mathrm{Mor}(V^m, V)$ of all polynomial maps from V^m to V with the algebra of $n \times n$ diagonal matrices with entries in $K[V^m]$ in the obvious way; then we have the usual trace function on $\mathrm{Mor}(V^m, V)$, and it is an algebra with trace in the sense of [32]. The special case $q = 1$ of Theorem 2.5 has the following corollary (by some methods of [31]): if $n!$ is invertible in K, then the algebra $\mathrm{Mor}_{S_n}(V^m, V)$ of S_n-equivariant polynomial maps from V^m to V is the trace-stable subalgebra generated by the generic diagonal matrices $x(1), \ldots, x(m)$ in the algebra of diagonal matrices with entries from $K[V^m]$. Furthermore, it is the free object of rank m in the category of commutative algebras with a trace satisfying the nth Cayley-Hamilton identity (in the sense of [32]). This latter result is due to Berele, see Theorem 2.1 in [3].

An element of $K[V^m]$ is *multilinear* if it is multihomogeneous with multidegree $(1, \ldots, 1)$. Define a multigrading on $\mathcal{F}(q)$ by setting the multidegree of $t(w)$ equal to the multidegree of w. The multilinear version of the above theorem is valid over an arbitrary base field. Abusing notation we keep on writing $K[V^m]^{G(n,q)}$ even if the group $G(n, q)$ is not defined over K (i.e. when K does not contain a primitive qth root of 1); in this case the notation refers to the algebra of invariants of S_n acting on the subalgebra of $K[V^m]$ spanned by monomials $u = u_{\langle 1 \rangle}^1 \cdots u_{\langle n \rangle}^n$, where $u^i \in \mathcal{M}(q) \cup \{1\}$ for all i (with the notation of the proof of Proposition 2.1).

Theorem 2.7. *Let K be an arbitrary field (or even an arbitrary commutative ring). Then the multilinear component of $K[V^m]^{G(n,q)}$ coincides with the multilinear component of the image of $\varphi(q)$. Moreover, any multilinear element in the kernel of $\varphi(q)$ is contained in the ideal generated by $\Psi(w_1, \ldots, w_{n+1})$, where $w_i \in \mathcal{M}(q)$ and the multidegree of $w_1 \cdots w_{n+1}$ belongs to $\{0, 1\}^m$.*

Proof. The only point in the proof of Proposition 2.1 where we need an assumption on K is to guarantee that $r_1! \cdots r_d! \neq 0$. If we consider multilinear elements of $K[V^m]$ only, then all the r_i here are automatically equal to 1. So the same argument yields that the multilinear elements in $K[V^m]$ of the form $[w_1] \cdots [w_r]$ (with $r \leq n$, $w_i \in \mathcal{M}(q)$) constitute a K-basis in the multilinear component of $K[V^m]^{G(n,q)}$. The relations from our statement are obviously sufficient to rewrite an arbitrary multilinear product of elements $[w]$ (with $w \in \mathcal{M}(q)$) as a linear combination of such products with at most n factors. This implies the claim. ∎

Remark 2.8. As an immediate corollary one recovers the known fact that the invariant $[x(1) \cdots x(m)] \in K[V^m]^{S_n}$ is indecomposable (can not be expressed by lower degree multisymmetric polynomials) when $0 < \mathrm{char}(K) \leq n$. Indeed, in this case each term of the fundamental relation is the product of at least two traces, hence there is no relation involving $[x(1) \cdots x(m)]$ as a term. This has interesting consequences for matrix invariants in positive characteristic, and for vector invariants of the orthogonal group; see [11].

3.   Finite presentation

Building on Derksen's general degree bound for syzygies in [9], we derive a finite presentation from Theorem 2.5.

Denote by $J_m(q)$ the ideal in $K[V^m]$ generated by the homogeneous $G(n, q)$-invariants of positive degree (the so-called Hilbert ideal), and denote by $\tau_{G(n,q)}(V^m)$ the minimal natural number d such that all homogeneous elements of degree $\geq d$ belong to $J_m(q)$.

Lemma 3.1. *We have $\tau_{G(n,q)}(V^m) = 1 + \sum_{j=1}^n (qj - 1)$.*

Proof. In the special case $q = 1$ (and $K = \mathbb{C}$, $m = 2$) this lemma appears

in [20] and is due to Wallach and Garsia. Define the *exponent* of a monomial $\prod_{i,j} x(i)_j^{\alpha_{ij}}$ as $(\beta_1, \ldots, \beta_n)$, where $\beta_j = \sum_{i=1}^m \alpha_{ij}$ (in other words, β_j is the exponent of x_j if we specialize all the $x(i)_j$ to x_j). Introduce a partial ordering on the set of monomials in $K[V^m]$: a monomial u is smaller than v if they have the same multidegree, and the exponent of u is lexicographically smaller than the exponent of v. This partial ordering is compatible with multiplication of monomials. We shall show that if $\beta_k \geq qk$ for some $k \in \{1, \ldots, n\}$, where $(\beta_1, \ldots, \beta_n)$ is the exponent of some monomial u in $K[V^m]$, then modulo $J_m(q)$, the monomial u can be rewritten as a linear combination of smaller monomials. We need some details from the proof of the special case $q = 1$ of our lemma. To simplify notation when $m = 1$, write $x_j = x(1)_j$. Then it is shown in Lemma 3.2.1 in [20] that

$$h_k(x_k, \ldots, x_n) \in J_1(1) \text{ for all } k = 1, \ldots, n, \tag{2}$$

where h_k denotes the kth complete symmetric polynomial of the arguments. Note that (2) shows that modulo $J_1(1)$, the monomial x_k^k can be rewritten as a linear combination of smaller monomials. Applying to (2) the comorphism of the S_n-equivariant morphism $V^m \to V$, $(v_1, \ldots, v_m) \mapsto v_1 + \cdots + v_m$ we get

$$h_k\left(\sum_{i=1}^m x(i)_k, \ldots, \sum_{i=1}^m x(i)_n\right) \in J_m(1) \text{ for all } k = 1, \ldots, n. \tag{3}$$

Since the ideal $J_m(1)$ is multihomogeneous, all multihomogeneous components of the left hand side of (3) belong to $J_m(1)$. In particular, for all $k = 1, \ldots, n$, there exists a linear combination f_k of k-linear monomials smaller than the monomial $x(1)_k x(2)_k \cdots x(k)_k$ such that

$$x(1)_k x(2)_k \cdots x(k)_k - f_k \in J_k(1). \tag{4}$$

(At this point it is essential that $k!$ is assumed to be invertible in K.) Now take an arbitrary k-tuple $w^{(1)}, \ldots, w^{(k)} \in \mathcal{M}(q)$. The map $x(i)_j \mapsto w_{\langle j \rangle}^{(i)}$ induces a K-algebra homomorphism $\gamma : K[V^k] \to K[V^m]^N$. Clearly γ is an S_n-equivariant map, whence $\gamma(J_k(1)) \subseteq J_m(q)$. Applying γ to (4) we get that

$$w_{\langle k \rangle}^{(1)} \cdots w_{\langle k \rangle}^{(k)} - \gamma(f_k) \in J_m(q), \tag{5}$$

where $\gamma(f_k)$ is a linear combination of monomials smaller than $w_{\langle k \rangle}^{(1)} \cdots w_{\langle k \rangle}^{(k)}$. Now let w be a monomial in the variables $x(1)_k, x(2)_k, \ldots, x(m)_k$ such that $\deg(w) = qk$. Then w can be factored as $w = w_{\langle k \rangle}^{(1)} \cdots w_{\langle k \rangle}^{(k)}$ with $w^{(i)} \in \mathcal{M}(q)$, whence modulo $J_m(q)$ the monomial w can be rewritten as a linear combination of smaller monomials by (5). This clearly implies that the factor space $K[V^m]/J_m(q)$ is spanned by the images of the monomials whose exponent $(\beta_1 \ldots, \beta_n)$ satisfies $\beta_k \leq qk - 1$ for all $k = 1, \ldots, n$. Since $J_m(q)$ is a homogeneous ideal, the factor space $K[V^m]/J_m(q)$ inherits the grading from $K[V^m]$. This shows that the homogeneous components of degree $> \sum_{k=1}^n (qk - 1)$ are all contained in $J_m(q)$, implying that $\tau_G(V^m) \leq 1 + \sum_{k=1}^n (qk - 1)$.

In the special case $m = 1$, the coordinate ring $K[V]$ is known to be a free module over $K[V]^{G(n,q)}$, and the latter is a polynomial algebra in n generators having degrees $q, 2q, \ldots, nq$. This implies a formula for the dimensions of the homogeneous components of the graded vector space $K[V]/J$, called the coinvariant algebra (see for example [7]). In particular, the highest degree non-zero homogeneous component has degree $\sum_{k=1}^{n}(qk - 1)$. This shows the reverse inequality $\tau_{G(n,q)}(V^m) \geq 1 + \sum_{k=1}^{n}(qk - 1)$. ∎

For a natural number d, consider the finitely generated subalgebra of $\mathcal{F}(q)$ given by

$$\mathcal{F}(q, d) = K[t(w) \mid w \in \mathcal{M}(q), \ \deg(w) \leq d].$$

Theorem 3.2.   *The kernel of the K-algebra surjection*

$$\mathcal{F}(q, qn(n+1) - 2n + 2) \to K[V^m]^G \text{ induced by } \quad t(w) \mapsto [w]$$

is generated as an ideal by the elements $\Psi(w_1, \ldots, w_{n+1})$, where $w_1, \ldots, w_{n+1} \in \mathcal{M}(q)$, and the degree of the product $w_1 \cdots w_{n+1}$ is not greater than $qn(n+1) - 2n + 2$.

Proof.   A general result of Derksen [9] says that the ideal of relations in a minimal presentation of $K[V^m]^G$ is generated in degree $\leq 2\tau_G(V^m)$. Therefore our statement follows from Theorem 2.5, Lemma 3.1, and the general Lemma 3.3 below. ∎

For a finitely generated commutative graded K-algebra A denote by $\tau(A)$ the minimal non-negative integer τ such that A and its first syzygy ideal are generated in degree τ. That is, let $\rho : K[x_1, \ldots, x_r] \to A$ be a surjective K-algebra homomorphism such that $\rho(x_i)$, $i = 1, \ldots, r$, is a minimal homogeneous generating system of A, and the grading on the polynomial algebra $K[x_1, \ldots, x_r]$ is defined so that ρ preserves the grading. Let $f_1, \ldots, f_s$ be a minimal homogeneous generating system of the ideal $\ker(\rho)$. Define

$$\tau(A) = \begin{cases} \max\{\deg(x_i) \mid i = 1, \ldots, r\}, & \text{if } \ker(\rho) = 0, \\ \max\{\deg(f_j) \mid j = 1, \ldots, s\} & \text{otherwise.} \end{cases}$$

Lemma 3.3.   *Let $\varphi : K[t_\mu \mid \mu \in M] \to A$ be a surjective homomorphism of graded algebras from a not necessarily finitely generated polynomial algebra, and let $\{f_\beta \mid \beta \in B\}$ be a homogeneous generating system of the ideal $\ker(\varphi)$. Then the kernel of the restriction of φ to the subalgebra $K[t_\mu \mid \deg(t_\mu) \leq \tau(A)]$ is generated as an ideal by $\{f_\beta \mid \deg(f_\beta) \leq \tau(A)\}$.*

Proof.   Denote by I the ideal of $R_1 = K[t_\mu \mid \deg(t_\mu) \leq \tau(A)]$ generated by $\{f_\beta \mid \deg(f_\beta) \leq \tau(A)\}$. Take a subset $C \subset M$ such that the restriction $\varphi_0 : R_0 = K[t_\mu \mid \mu \in C] \to A$ of φ is a minimal presentation of A. Then $\ker(\varphi_0)$ is generated in degree $\tau(A)$ and is contained in $\ker(\varphi) = (f_\beta \mid \beta \in B)$, hence $\ker(\varphi_0) \subset I$. Moreover, since $\operatorname{im}(\varphi_0) = \operatorname{im}(\varphi)$, for each $\mu \in M$ there is an element $g_\mu \in R_0$ with $\deg(t_\mu) = \deg(g_\mu)$ such that $t_\mu - g_\mu \in \ker(\varphi)$. Obviously,

if $\deg(t_\mu) \leq \tau(A)$, then $t_\mu - g_\mu \in I$. It follows that $R_1 = R_0 + I$, implying $\ker(\varphi_1) = \ker(\varphi_0) + I = I$. ∎

Remark 3.4. Since the Hilbert ideal of a subgroup H of $G(n, q)$ contains the Hilbert ideal of $G(n, q)$, we have $\tau_H(V^m) \leq \tau_{G(n,q)}(V^m)$. Thus Lemma 3.1 provides upper bounds on the degrees of the relations in a minimal presentation of $K[V^m]^H$ by the result of Derksen [9] cited above. Among subgroups of $G(n, q)$ are other series of pseudo-reflection groups, including the Weyl groups of type D_n or the dihedral groups.

4.   Semisimple commutative representations

In this section we work over the field $\mathbb{C}$ of complex numbers (what is essential for Theorem 4.1 is that the base field has characteristic zero). Write F_m for the free associative algebra $\mathbb{C}\langle x_1, \ldots, x_m\rangle$, and A_m for the commutative polynomial algebra $\mathbb{C}[x(1), \ldots, x(m)]$. Denote by $\mathrm{rep}(F_m, n)$ the space of m-tuples of complex $n \times n$ matrices, endowed with the simultaneous conjugation action of $GL(n, \mathbb{C})$. The points of this affine variety determine n-dimensional representations of F_m in the obvious way, and the $GL(n, \mathbb{C})$-orbits are in a one-to-one correspondence with the isomorphism classes of n-dimensional representations of F_m. The algebraic quotient $\mathrm{rep}(F_m, n)//GL(n, \mathbb{C})$ parameterizes the isomorphism classes of semisimple n-dimensional representations of the free algebra, see [2]. The coordinate ring $\mathbb{C}[\mathrm{rep}(F_m, n)]$ is the n^2m-variable polynomial algebra generated by the entries of the generic $n \times n$ matrices $Y(1), \ldots, Y(m)$. Denote by J the ideal in $\mathbb{C}[\mathrm{rep}(F_m, n)]$ generated by the entries of the commutators $Y(i)Y(j) - Y(j)Y(i)$, $1 \leq i < j \leq m$. The quotient algebra $\mathbb{C}[\mathrm{rep}(F_m, n)]/J = \mathbb{C}[\mathrm{rep}(A_m, n)]$ is the coordinate ring of the *scheme* $\mathrm{rep}(A_m, n)$ *of n-dimensional representations of A_m* (by definition of this affine scheme). It is a long standing open problem in commutative algebra whether this scheme is reduced or not, or equivalently, whether J is a radical ideal or not; see for example [21]. The common zero locus of J (i.e. the set of $\mathbb{C}$-points of the scheme $\mathrm{rep}(A_m, n)$) is the so-called *commuting variety* consisting of m-tuples of pairwise commuting $n \times n$-matrices. So the question is whether J is the whole vanishing ideal of the commuting variety or not. The embedding of the space V^m of m-tuples of diagonal matrices into the commuting variety induces a surjective homomorphism $\beta : \mathbb{C}[\mathrm{rep}(A_m, n)] \to \mathbb{C}[V^m]$. Consider the homomorphism $\gamma : \mathcal{F}(1) \to \mathbb{C}[\mathrm{rep}(A_m, n)]^{GL(n,\mathbb{C})}$ given by $t(w) \mapsto \mathrm{Tr}(Y(1)^{\alpha_1} \cdots Y(m)^{\alpha_m})$ for $w = x(1)^{\alpha_1} \cdots x(m)^{\alpha_m} \in \mathcal{M}(1)$, where we keep the notation $Y(j)$ for the images of the generic matrices under the natural surjection

$$M(n, \mathbb{C}[\mathrm{rep}(F_m, n)]) \to M(n, \mathbb{C}[\mathrm{rep}(A_m, n)]).$$

It is well known that γ is surjective, see [38]; we use here that any $GL(n, \mathbb{C})$-invariant in $\mathbb{C}[\mathrm{rep}(A_m, n)]$ lifts to an invariant on $\mathrm{rep}(F_m, n)$, since our base field has characteristic zero. The fundamental trace identity holds in $M(n, C)$ for an arbitrary commutative ring C (this is equivalent to the Cayley-Hamilton theorem), therefore $\Psi(w_1, \ldots, w_{n+1}) \in \ker(\gamma)$ for any $w_i \in \mathcal{M}(1)$. It follows by Theorem 2.5 that γ factors through a surjection

$$\overline{\gamma} : \mathbb{C}[V^m]^{S_n} \to \mathbb{C}[\mathrm{rep}(A_m, n)]^{GL(n,\mathbb{C})}, \quad [w] \mapsto \mathrm{Tr}(Y(1)^{\alpha_1} \cdots Y(m)^{\alpha_m})$$

for $w = x(1)^{\alpha_1} \cdots x(m)^{\alpha_m} \in \mathcal{M}(1)$. So we have the surjections

$$\mathbb{C}[V^m]^{S_n} \xrightarrow{\overline{\gamma}} \mathbb{C}[\mathrm{rep}(A_m, n)]^{GL(n,\mathbb{C})} \xrightarrow{\beta} \mathbb{C}[V^m]^{S_n}.$$

Since $\beta \circ \overline{\gamma}$ is the identity map of $\mathbb{C}[V^m]^{S_n}$ by definition of the maps $\overline{\gamma}$ and β, we conclude that they are isomorphisms. Thus we obtained the following result, supporting the conjecture that the commuting scheme is reduced:

Theorem 4.1. *The surjection $\mathbb{C}[\mathrm{rep}(A_m, n)] \to \mathbb{C}[V^m]$ induced by the embedding of the space of m-tuples of diagonal matrices into the commuting variety restricts to an isomorphism $\mathbb{C}[\mathrm{rep}(A_m, n)]^{GL(n,\mathbb{C})} \cong \mathbb{C}[V^m]^{S_n}$. In particular, the radical of $\mathbb{C}[\mathrm{rep}(A_m, n)]$ contains no non-zero $GL(n,\mathbb{C})$-invariants.*

Remark 4.2. One may paraphrase the above theorem by saying that "the scheme of n-dimensional semisimple representations of the commutative m-variable polynomial algebra is reduced". (The weaker statement that the algebraic quotient of the commuting variety with respect to the action of $GL(n,\mathbb{C})$ is isomorphic to V^m/S_n is well known, and is explained for example in Proposition 6.2.1 of [20].) In the special case $m = 2$, reducedness of $\mathbb{C}[\mathrm{rep}(A_m, n)]^{GL(n,\mathbb{C})}$ was proved by different methods by Gan and Ginzburg, see Theorem 1.2.1 in [19]. For arbitrary m it appeared in our preprint [12], and is proved also by Vaccarino in his parallel preprint [arXiv:math.AG/0602660], that appeared in the meantime as [42].

5. Multisymmetric functions over an arbitrary base ring

Throughout this section K is an arbitrary base ring. We extend the method of Section 2 to this case.

For a monomial $w \in \mathcal{M} = \mathcal{M}(1)$ and $l \in \{1, \dots, n\}$ we set

$$\sigma_l(w) = \sum_{1 \leq i_1 < \cdots < i_l \leq n} w_{\langle i_1 \rangle} \cdots w_{\langle i_l \rangle}.$$

In other words, $\sigma_l(w)$ is the lth coefficient of the characteristic polynomial of the diagonal matrix w. By the multiset $\{w_1, \dots, w_d; r_1, \dots, r_d\}$ of monomials from $\mathcal{M}$ we mean the multiset which contains d distinct monomials $w_1, \dots, w_d$, and the multiplicity of w_i is r_i.

Proposition 5.1. *A free K-module basis in $K[V^m]^{S_n}$ is formed by the products $\sigma_{r_1}(w_1) \cdots \sigma_{r_d}(w_d)$, where $\{w_1, \dots, w_d; r_1, \dots, r_d\}$ range over all multisets of monomials from $\mathcal{M}$ with $r_1 + \cdots + r_d \leq n$.*

Proof. The proof is essentially the same as that of Proposition 2.1: when we expand $\sigma_{r_1}(w_1) \cdots \sigma_{r_d}(w_d)$ as a linear combination of monomial multisymmetric functions, the coefficient of $O_{\{w_1, \dots, w_d; r_1, \dots, r_d\}}$ is 1, and all other monomial multisymmetric functions contributing have strictly smaller height. This implies the claim, since the $O_{\{w_1, \dots, w_d; r_1, \dots, r_d\}}$ with $r_1 + \cdots + r_d \leq n$ form a K-basis in $K[V^m]^{S_n}$. ∎

In particular, the K-algebra $K[V^m]^{S_n}$ is generated by the $\sigma_r(w)$. Our aim is to determine generators of the ideal of relations among these generators. With

$w \in \mathcal{M}$ and $r \in \{1, \ldots, n\}$ associate a commuting indeterminate $e_r(w)$, and denote by

$$\phi : K[e_r(w) \mid w \in \mathcal{M}, r = 1, \ldots, n] \to K[V^m]^{S_n}$$

the K-algebra surjection induced by $e_r(w) \mapsto \sigma_r(w)$.

Denote by σ_l^α the multidegree $\alpha = (\alpha_1, \ldots, \alpha_s)$ multihomogeneous component of the lth characteristic coefficient of the diagonal matrix $x(1) + \cdots + x(s)$ (note that necessarily $l = \alpha_1 + \cdots + \alpha_s$). Specializing Amitsur's formula [1] for the characteristic coefficients of a linear combination of matrices one obtains formula (6) below. To state it we need to introduce some integers. Take non-commuting variables $Y_1, \ldots, Y_s$, and consider $\mathcal{W}$, the semigroup of words in $Y_1, \ldots, Y_s$. The word U is *reduced* if it is not a power U_0^k for some $k \geq 2$ and shorter word U_0. The words $U_1 U_2$ and $U_2 U_1$ are said to be *cyclically equivalent*. Write $\mathcal{W}_0$ for the set of cyclic equivalence classes of reduced words. Denote by $C_{\{(r_1,u_1),\ldots,(r_d,u_d)\}}$ the number of multisets $\{U_1, \ldots, U_d; r_1, \ldots, r_d\}$ of cyclic equivalence classes of reduced words (so $U_1, \ldots, U_d$ are distinct elements of $\mathcal{W}_0$, with multiplicities $r_1, \ldots, r_d$) such that the specialization $Y_i \mapsto x(i)$ $(i = 1, \ldots, m)$ sends U_j to u_j $(j = 1, \ldots, d)$; note that non-commuting reduced words from different cyclic equivalence classes may specialize to the same commuting monomial, so here $\{(r_1, u_1), \ldots, (r_d, u_d)\}$ is a multiset of pairs (i.e. (r_i, u_i) and (r_j, u_j) may be equal for $i \neq j$), where $u_i \in \mathcal{M}_s$, the set of commuting monomials in $x(1), \ldots, x(s)$ (we need to allow $s > m$). By [1] we have

$$\sigma_l^\alpha = \sum (-1)^{l+r_1+\cdots+r_d} C_{\{(r_1,u_1),\ldots,(r_d,u_d)\}} \sigma_{r_1}(u_1) \cdots \sigma_{r_d}(u_d), \qquad (6)$$

where the summation ranges over multisets of pairs $\{(r_1, u_1), \ldots, (r_d, u_d)\}$, where $r_i \in \mathbb{N}$, $u_i \in \mathcal{M}_s$ with multidegree $\mathrm{multideg}(u_1^{r_1} \cdots u_d^{r_d}) = \alpha$. Extending the definition of σ by setting $\sigma_l = 0$ for $l > n$, the equality (6) remains valid also if $l > n$. For a multidegree $\alpha = (\alpha_1, \ldots, \alpha_s)$ and $w_1, \ldots, w_s \in \mathcal{M}$ define

$$S^\alpha(w_1, \ldots, w_s) \in K[e_r(w) \mid w \in \mathcal{M}, r = 1, \ldots, n]$$

as the element obtained by making first the substitution $x(i) \mapsto w_i$, $i = 1, \ldots, s$ in the right hand side of (6), and replacing the symbols σ by e everywhere. Since σ_l is identically zero for $l > n$, the equality (6) shows that

$$S^\alpha(w_1, \ldots, w_s) \in \ker(\phi) \quad \text{if } \sum \alpha_i > n. \qquad (7)$$

There is another type of relations we shall need. Simplify the notation by writing $x = x(1)$ in the special case $m = 1$. It is well known that $K[V]^{S_n}$ is generated by the algebraically independent elements $\sigma_r(x)$, $r = 1, \ldots, n$, hence for each $k \geq 2$ and $j \in \{1, \ldots, n\}$ there is a unique n-variable polynomial $f_{j,k}$ with integer coefficients such that $\sigma_j(x^k) = f_{j,k}(\sigma_1(x), \ldots, \sigma_n(x))$. Now given a monomial $w \in \mathcal{M}$, consider the element

$$Q_{j,k}(w) = e_j(w^k) - f_{j,k}(e_1(w), \ldots, e_n(w)) \in \ker(\phi).$$

For example, it is an easy exercise to verify that

$$Q_{r,2}(x) = e_r(x^2) - \sum_{i=\max\{0,2r-n\}}^{\min\{2r,n\}} (-1)^{r+i} e_i(x) e_{2r-i}(x).$$

As a first application of the relations (7) we derive a short proof of the degree bound of Fleischmann [16] for the generators of $K[V^m]^{S_n}$. We call an element of $K[V^m]^{S_n}$ *indecomposable* if it is not contained in the K-subalgebra generated by strictly lower degree elements, and call it *decomposable* otherwise. Obviously, a homogeneous element of $K[V^m]^{S_n}$ is indecomposable if and only if it is not contained in the square $\mathcal{A}^2$ of the ideal $\mathcal{A}$ of $K[V^m]^{S_n}$ spanned by the homogeneous components of positive degree.

Lemma 5.2.   *Let $w = x(1)^{\alpha_1} \cdots x(m)^{\alpha_m} \in \mathcal{M}$ be a monomial such that $\alpha_j \geq n/r$ for some j, and $\deg(w) \geq 1 + n/r$. Then $\sigma_r(w)$ is decomposable.*

Proof.   Apply induction on r. Clearly it is sufficient to show that if $kr \geq n$, then $\sigma_r(x^k y) \in \mathcal{A}^2$ (here we write x, y instead of $x(1), x(2)$). Indeed, the general case follows on substituting x, y by appropriate monomials. ¿From the relation $\phi(S^{(kr,r)}(x,y)) = 0$ we get

$$(-1)^r \sigma_r(x^k y) + \sum (-1)^{r/i} C_{\{x^{ki}y^i\}} \sigma_{r/i}(x^{ki} y^i) \in \mathcal{A}^2,$$

where the sum ranges over divisors $i > 1$ of r (and $C_{\{x^{ki}y^i\}}$ is the number of cyclic equivalence classes of reduced words that specialize to $x^{ki}y^i$). In particular, this sum is empty if $r = 1$ and so $\sigma_1(x^k y) \in \mathcal{A}^2$ for $k \geq n$. If $r > 1$, then the assumptions in our lemma apply to all summands, hence they belong to $\mathcal{A}^2$ by the induction hypothesis, forcing $\sigma_r(x^k y) \in \mathcal{A}^2$.   ∎

Corollary 5.3.   *The K-algebra $K[V^m]^{S_n}$ is generated by the elements $\sigma_n(x(i))$, $i \in \{1, \ldots, m\}$, and $\sigma_r(x(1)^{\alpha_1} \cdots x(m)^{\alpha_m})$, where $r \in \{1, \ldots, n\}$, $\alpha_j < n/r$ for all $j = 1, \ldots, m$, and the greatest common divisor of $\alpha_1, \ldots, \alpha_m$ is 1.*

Remark 5.4.   In particular, $K[V^m]^{S_n}$ is generated in
$$\text{degree} \leq \max\{m(n-1), n\};$$
this is the main result of Fleischmann [16], where it is also shown that this bound can not be improved in general. Using the method of [16] we showed in [11] that if K is a field of characteristic p and $n = p^k$ with $k \in \mathbb{N}$, then $\sigma_{n-1}(x(1) \cdots x(m))$ is indecomposable. Vaccarino [41] shows that the $\sigma_r(w)$ with w reduced (not a power of a monomial with lower degree) generate the ring of multisymmetric functions, and refering to the bound from [16] deduces a finite system of generators. Our Corollary 5.3 reduces further this generating system. A minimal generating system of $K[V^m]^{S_n}$ appears in [35].

Theorem 5.5.   *The ideal $\ker(\phi)$ is generated by*

$$S^\alpha(w_1, \ldots, w_s) \qquad and \qquad Q_{r,k}(w),$$

where $s \geq 2$, $w, w_1, \ldots, w_s \in \mathcal{M}$; $\sum_{i=1}^s \alpha_i > n$, $\sum_{i \neq j} \alpha_i \leq n$ for all $j = 1, \ldots, s$; $r \in \{1, \ldots, n\}$; $k < 1 + n/r$.

Proof.   Call the *weight* of a product $\sigma_{r_1}(w_1) \cdots \sigma_{r_s}(w_s)$ the integer $r_1 + \cdots + r_s$. First we show that if the weight is $> n$, then modulo the first type relations in our

statement, this product can be rewritten as a linear combination of products with strictly smaller weight. It is sufficient to deal with the case when $\sum_{i \neq j} r_i \leq n$ for all $j = 1, \ldots, s$. Set $\alpha = (r_1, \ldots, r_s)$. Then $S^\alpha(x(1), \ldots, x(s))$ contains the term $e_{r_1}(x(1)) \cdots e_{r_s}(x(s))$ with coefficient ± 1. In any other term $e_{i_1}(u_1) \cdots e_{i_d}(u_d)$ of S^α, at least one of the u_t has degree > 1, hence $i_1 + \cdots + i_d < r_1 + \cdots + r_s$. So the relation $\phi(S^\alpha(w_1, \ldots, w_s)) = 0$ does what we need.

Next we claim that using our relations, any product $\sigma_{r_1}(w_1) \cdots \sigma_{r_d}(w_d)$ with weight $\leq n$ can be rewritten as a linear combination of $\sigma_{i_1}(u_1) \cdots \sigma_{i_t}(u_t)$ with weight $\leq \sum r_i$ and $u_1, \ldots, u_t$ distinct. By Proposition 5.1 our theorem will follow. Obviously, it is sufficient to verify the latter claim in the special case when all the w_i are powers of the same monomial w. We may also assume that $w = x$, so we are working in the special case $m = 1$. An inspection of the proof of Proposition 5.1 shows that $\sigma_{r_1}(x^{j_1}) \cdots \sigma_{r_d}(x^{j_d})$ is a linear combination of monomial multisymmetric functions of height $\leq \sum r_i$, and in the K-space spanned by such monomial multisymmetric functions, the products $\sigma_{i_1}(x^{k_1}) \cdots \sigma_{i_t}(x^{k_t})$ with weight $\leq \sum r_i$ and $k_1, \ldots, k_t$ distinct form a basis. So we conclude that there are relations among the $\sigma_r(x^k)$ of the desired form. Therefore it suffices to prove the special case $m = 1$ of our theorem.

Since in the special case $m = 1$, $K[V]^{S_n}$ is a polynomial ring generated by $\sigma_1(x), \ldots, \sigma_n(x)$, all we need to show is that our relations are sufficient to express all $\sigma_r(x^k)$ in terms of the n algebraically independent generators. We apply a double induction: the first induction goes on $\deg(\sigma_r(x^k)) = rk$, and the second induction goes on r. If $(k-1)r < n$, then we may use our relation $\phi(Q_{r,k}(x)) = 0$ from our statement and we are done. Assume $(k-1)r \geq n$. Then we slightly adjust the argument in the proof of Lemma 5.2. Write l for the lower integral part of n/r. Then we have $k > l$ and we have the relation $\phi(S^{(lr,r)}(x, x^{k-l})) = 0$ in our statement. This relation can be used to express

$$(-1)^r \sigma_r(x^k) + \sum (-1)^{r/i} C_{\{x^{li}y^i\}} \sigma_{r/i}(x^{ki})$$

(where the sum ranges over divisors $i > 1$ of r) by lower degree elements. The statement then follows by the two induction hypotheses. ∎

Remark 5.6. Although the above theorem is far from yielding a finite presentation of $K[V^m]^{S_n}$, at least it gives a uniform presentation in the sense that all relations are obtained from finitely many types by substituting different monomials (note that the restrictions made on α force $\sum_{i=1}^s \alpha_i \leq 2n$ and $s \leq n+1$). For comparison we mention that in [41] the author considers the generating system $\sigma_r(w)$ where w is reduced (i.e. is not a power of a monomial with smaller degree), and describes the relations among these generators in the following sense: he works in the ring of multisymmetric functions in infinitely many variables, where the analogues of $\sigma_r(w)$ ($r \in \mathbb{N}$, $w \in \mathcal{M}$ reduced) form an algebraically independent generating system, and observes that the unique expressions of the monomial multisymmetric functions with height $> n$ in terms of these generators form a K-basis in the space of relations among these generators. Implementing this procedure in practice one needs to produce formulae like our $Q_{r,k}(w)$ but with no bound on r and k, and one needs to produce expressions similar to $S^\alpha(w_1, \ldots, w_s)$ with no

bound on α.

6.   Calculations

Throughout this section we assume that $n!$ is invertible in K, so $K[V^m]^{S_n}$ is Cohen-Macaulay (see for example [10] as a general reference for the invariant theory of finite groups). To illustrate how to proceed to find a minimal presentation we do calculations in concrete examples. An obvious homogeneous system of parameters *(primary generators)* in $K[V^m]^{S_n}$ is

$$P = \{[x(i)], [x(i)^2], \ldots, [x(i)^n] \mid i = 1, \ldots, m\}.$$

Write $\langle P \rangle$ for the ideal of $K[V^m]^{S_n}$ generated by P, and write $K[P]$ for the polynomial subalgebra of $K[V^m]^{S_n}$ generated by P. Note that to find *secondary generators* we need to get a vector space basis modulo $\langle P \rangle$ in $K[V^m]^{S_n}$.

Lemma 6.1.   *Assume that $n!$ is invertible in K. Let w be a monomial having degree $\geq n$ in one of the variables $x(1), \ldots, x(m)$, and having total degree $\geq n+1$. Then $[w]$ belongs to $\langle P \rangle$.*

Proof.   Assume for example that w has degree $\geq n$ in $x(1)$. Then w can be written as a product of $n + 1$ factors as $x(1)x(1)\cdots x(1)u$ for some non-empty monomial u. The relation $\Psi_{n+1}(x(1), x(1), \ldots, x(1), u) = 0$ shows the claim, since each nontrivial partition of the multiset $\{x(1), \ldots, x(1), u\}$ contains a part consisting solely of $x(1)$s.   ∎

Remark 6.2.   From Lemma 6.1 and Proposition 2.1 we immediately get the upper bound $n(n-1)m$ for the degrees of the secondary generators. However, the general method of Broer (see Theorem 3.9.8 in [10]) yields the better bound $\frac{1}{2}n(n-1)m$.

6.1. The case $n = 2$

In this subsection we assume $\mathrm{char}(K) \neq 2$. The fundamental multilinear trace identity for diagonal 2×2 matrices is

$$[xyz] = \frac{1}{2}([xy][z] + [xz][y] + [yz][x] - [x][y][z]) \tag{8}$$

Substitute $z \mapsto zw$ in (8), and eliminate traces of degree 3 using (8) to get

$$[xyzw] = \frac{1}{4}([xz][y][w] + [xw][y][z] + [yz][x][w] + [yw][x][z])$$

$$+\frac{1}{2}[xy][zw] - \frac{1}{2}[x][y][z][w] \tag{9}$$

Exchanging the variables y and z in (9) we obtain

$$[xzyw] = \frac{1}{4}([xy][z][w] + [xw][y][z] + [yz][x][w] + [zw][x][y])$$

$$+\frac{1}{2}[xz][yw] - \frac{1}{2}[x][y][z][w] \tag{10}$$

The difference of (9) and (10) yields

$$[xz][yw] - [xy][zw] = \frac{1}{2}([xy][z][w] + [zw][x][y] - [xz][y][w] - [yw][x][z]) \qquad (11)$$

(compare with (4.17) in [30]). The specialization $z = w$ in (11) leads to

$$[xz][yz] = [xy][zz] + \frac{1}{2}([xy][z][z] + [zz][x][y] - [xz][y][z] - [yz][x][z]) \qquad (12)$$

The $\mathbb{N}_0^m$-graded Hilbert series of $K[V^m]^{S_2}$ can be written as a rational function by Molien's formula:

$$H(K[V^m]^{S_2}; t_1, \ldots, t_m) = \frac{\sum_{i=0}^{[\frac{m}{2}]} e_{2i}(t_1, \ldots, t_m)}{\prod_{j=1}^{m}(1 - t_j)(1 - t_j^2)},$$

where $e_i(t_1, \ldots, t_m)$ is the ith elementary symmetric function in $t_1, \ldots, t_m$. It is easy to describe the Hironaka decomposition of $K[V^m]^{S_2}$. The secondary generators are

$$S = \{[x(i_1)x(i_2)] \cdots [x(i_{2k-1})x(i_{2k})] \mid 1 \le i_1 < \cdots < i_{2k} \le m\}.$$

The substitution $x \mapsto x(i)$, $y \mapsto x(j)$, $z \mapsto x(k)$ in (12) gives a relation showing that $[x(i)x(k)][x(j)x(k)]$ is contained in $\langle P \rangle$ for all i, j, k. Substitutions $\{x, y, z, w\} \to \{x(j_1), \ldots, x(j_{2k})\}$ in the relation (11) show that

$$[x(j_1)x(j_2)] \cdots [x(j_{2k-1})x(j_{2k})] - [x(j_{\pi(1)})x(j_{\pi(2)})] \cdots [x(j_{\pi(2k-1)})x(j_{\pi(2k)})]$$

belongs to $\langle P \rangle$ for an arbitrary permutation π. These relations imply that the algebra of multisymmetric functions is generated by S as a module over the polynomial ring $K[P]$. The Hilbert series shows that it is a free module. These considerations show also that the specializations $\{x, y, z, w\} \to \{x(1), \ldots, x(m)\}$ in (11) generate the ideal of relations among the generators $[x(i)], [x(k)x(l)]$, and that a minimal system of relations consists of relations of degree 4.

6.2. The case $n = 3$, $m = 2$

In this subsection we assume $\mathrm{char}(K) \ne 2$ and $\mathrm{char}(K) \ne 3$. The fundamental identity $\Psi_4(x, y, z, w) = 0$ takes the form

$$[xyzw] = \frac{1}{3}([xyz][w] + [xyw][z] + [xzw][y] + [yzw][x])$$

$$+ \frac{1}{6}([xy][zw] + [xz][yw] + [xw][yz] + [x][y][z][w])$$

$$- \frac{1}{6}([xy][z][w] + [xz][y][w] + [xw][y][z] +$$
$$+ [yz][x][w] + [yw][x][z] + [zw][x][y])$$

Consider the following consequences:

$$\begin{array}{lll}
\Psi_4(x, x, x, x) = 0 & \Psi_4(y, y, y, y) = 0 & \Psi_4(x, x, x, y) = 0 \qquad (13) \\
\Psi_4(y, y, y, x) = 0 & \Psi_4(x, x, x, xy) = 0 & \Psi_4(y, y, y, xy) = 0 \\
\Psi_4(x, x, y, y) = 0 & \Psi_4(x, x, x, y^2) = 0 & \Psi_4(y, y, y, x^2) = 0 \\
\Psi_4(x, x, x, y^3) = 0 & \Psi_4(x, x, x, xy^2) = 0 & \Psi_4(y, y, y, yx^2) = 0
\end{array}$$

and

$$\Psi_4(x^2, x, y, y) = 0 \qquad \Psi_4(y^2, y, x, x) = 0 \tag{14}$$
$$\Psi_4(x^2, x^2, y, y) = 0 \qquad \Psi_4(y^2, y^2, x, x) = 0$$
$$\Psi_4(x^2, x, y^2, y) = 0$$

Let us use the notation $f \equiv g$ to indicate that $f, g \in K[V^2]^{S_3}$ are congruent modulo $\langle P \rangle$. The above 17 relations in the order of listing imply the following:

$$[x^4] \equiv 0 \qquad [y^4] \equiv 0 \qquad [x^3 y] \equiv 0$$
$$[xy^3] \equiv 0 \qquad [x^4 y] \equiv 0 \qquad [xy^4] \equiv 0$$
$$[x^2 y^2] \equiv \tfrac{1}{3}[xy][xy] \qquad [x^3 y^2] \equiv 0 \qquad [y^3 x^2] \equiv 0$$
$$[x^3 y^3] \equiv 0 \qquad [x^4 y^2] \equiv 0 \qquad [y^4 x^2] \equiv 0$$

and

$$[x^3 y^2] \equiv \tfrac{1}{3}[x^2 y][xy] \qquad [y^3 x^2] \equiv \tfrac{1}{3}[y^2 x][yx]$$
$$[x^4 y^2] \equiv \tfrac{1}{3}[x^2 y][x^2 y] \qquad [x^2 y^4] \equiv \tfrac{1}{3}[xy^2][xy^2]$$
$$[x^3 y^3] \equiv \tfrac{1}{6}[x^2 y][xy^2] + \tfrac{1}{6}[x^2 y^2][xy]$$

Recall that $K[V^2]^{S_3}$ is minimally generated as an algebra by $P \cup \{[xy], [x^2 y], [xy^2]\}$. The above congruences obviously show that as a module over $K[P]$, the algebra $K[V^2]^{S_3}$ is spanned by

$$S = \{1, [xy], [x^2 y], [xy^2], [xy]^2, [x^2 y][xy^2]\}.$$

Using Molien's formula one can easily compute

$$H(K[V^2]^{S_3}; t_1, t_2) = \frac{1 + t_1 t_2 + t_1^2 t_2 + t_1 t_2^2 + t_1^2 t_2^2 + t_1^3 t_2^3}{(1 - t_1)(1 - t_1^2)(1 - t_1^3)(1 - t_2)(1 - t_2^2)(1 - t_2^3)},$$

and this implies that $K[V^2]^{S_3}$ is a free $K[P]$-module generated by S. The above considerations imply that the ideal of relations among the 21 generators

$$\{[x^i y^j] \mid 0 \le i, j \le 4, \quad i + j \le 6, \quad (i, j) \ne (0, 0)\}$$

is generated by the 17 relations (13) and (14). The relations (13) can be used to eliminate the 12 superfluous generators of degree ≥ 4 in the relations (14). This way we get 5 defining relations for the minimal generating system

$$\{[x^i y^j] \mid i + j \le 3\}.$$

The bidegrees of these relations are $(3, 2)$, $(2, 3)$, $(4, 2)$, $(2, 4)$, $(3, 3)$. It is easy to see that these 5 relations minimally generate the ideal of relations. (In subsequent work, the minimal presentation of $\mathbb{C}[V^m]^{S_3}$ is determined in [14] for arbitrary m.)

References

[1]   Amitsur, S. A., *On the characteristic polynomial of a sum of matrices*, Lin. Multilin. Alg. **8** (1980), 177–182.

[2]   Artin, M., *On Azumaya algebras and finite dimensional representations of rings*, J. Algebra **11** (1969), 532–563.

[3]   Berele, A., *Trace identities for diagonal and upper triangular matrices*, International J. Algebra and Computation **6** (1996), 645–654.

[4]   Berele, A., and A. Regev, *Some results on trace cocharacters*, J. Algebra **176** (1995), 1013–1024.

[5]   Briand, E., *When is the algebra of multisymmetric polynomials generated by the elementary multisymmetric polynomials?*, Beiträge Algebra Geom. **45** (2004), 353–368.

[6]   Bukhshtaber, V. M., and E. G. Rees, *Rings of continuous functions, symmetric products, and Frobenius algebras, (in Russian)*, Uspekhi Mat. Nauk **59** (2004), 125–144.

[7]   Chevalley, C., *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782.

[8]   Dalbec, J., *Multisymmetric functions*, Beiträge Algebra Geom. **40** (1999), 27–51.

[9]   Derksen, H., *Degree bounds for syzygies of invariants*, Adv. Math. **185** (2004), 207–214.

[10]   Derksen, H., and G. Kemper, "Computational invariant theory," Springer-Verlag, Berlin, 2002.

[11]   Domokos, M., *Matrix invariants and the failure of Weyl's theorem*, in: A. Giambruno, A. Regev, M. Zaicev, Eds., "Polynomial identities and combinatorial methods", Lecture Notes in Pure and Applied Mathematics **235**, Marcel Dekker, 2003, 215–236.

[12]   —, *Multisymmetric syzygies*, arXiv:math.RT/0602303.

[13]   —, *Fundamental theorems for invariants of a class of pseudo-reflection groups*, arXiv:math.RT/0611430.

[14]   Domokos, M., and A. Puskás, *Multisymmetric polynomials in dimension three*, in preparation.

[15]   Feshbach, M., *The mod 2 cohomology rings of the symmetric groups and invariants*, Topology **41** (2002), 57–84.

[16]   Fleischmann, P., *A new degree bound for vector invariants of symmetric groups*, Trans. Amer. Math. Soc. **350** (1998), 1703–1712.

[17] —, *On invariant theory of finite groups*, in: H. E. A. Campbell, D. L. Wehlau, Eds., "Invariant theory in all characteristics," CRM Proceedings and Lecture Notes **35**, Amer. Math. Soc., 2004, 43–69.

[18] Formanek, E., "The polynomial identities and invariants of $n \times n$ matrices," Regional Conference Series in Mathematics **78**, American Math. Soc., 1991.

[19] Gan, W. L., and V. Ginzburg, *Almost-commuting variety, D-modules, and Cherednik algebras*, Int. Math. Research Papers **2006:2** (2006), 1-54.

[20] Haiman, M. D., *Conjectures on the quotient ring by diagonal invariants*, J. Algebraic Combin. **3** (1994), 17–76.

[21] Hreinsdottir, F., *Conjectures on the ring of commuting matrices*, arXiv:math.AC/0501465.

[22] Hunziker, M., *Classical invariant theory for finite reflection groups*, Transformation Groups **2** (1997), 147–163.

[23] Jerjen, H., "Weitere Ergebnisse zur allgemeinen Vermutung in der Invariantentheorie von endlichen Spiegelungsgruppen," Diplomarbeit, Universität Basel, Basel, Switzerland, 1989.

[24] Junker, Fr., *Die Relationen, welche zwischen den elementaren symmetrischen Functionen bestehen*, Math. Ann. **38** (1891), 91–114.

[25] —, *Ueber symmetrische Functionen von mehreren Reihen von Veränderlichen*, Math. Ann. **43** (1893), 225–270.

[26] —, *Die symmetrischen Functionen und die Relationen zwischen den Elementarfunctionen derselben*, Math. Ann. **45** (1894), 1–84.

[27] Kemer, A., *Multilinear identities of the algebras over a field of characteristic p*, International J. Algebra and Computation **5** (1995), 189–197.

[28] MacMahon, P. A., "Combinatory analysis, Vol II", Cambridge Univ. Press, 1916.

[29] Noether, E., *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1915), 89–92.

[30] Olver, P. J., "Classical Invariant Theory", Cambridge University Press, 1999.

[31] Procesi, C., *The invariant theory of $n \times n$ matrices*, Adv. Math. **19** (1976), 306–381.

[32] —, *A formal inverse to the Cayley-Hamilton theorem*, J. Algebra **107** (1987), 63–74.

[33] Razmyslov, Yu. P., *Trace identities of full matrix algebras over a field of characteristic zero, (in Russian)*, Izv. Akad. Nauk. SSSR Ser. Mat. **38** (1974), 723–756.

[34] Richman, D. R., *Explicit generators of the invariants of finite groups*, Adv. Math. **124** (1996), 49–76.

[35] Rydh, D., *A minimal set of generators for the ring of multisymmetric functions*, Ann. Inst. Fourier (Grenoble) **57** (2007), 1741–1769.

[36] Schläfli, L., *Über die Resultante eines Systemes mehrerer algebraischer Gleichungen*, Vienna Academy Denkschriften **4** (1852).

[37] Shephard, G. C., and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.

[38] Sibirskiĭ, K. S., *Algebraic invariants for a set of matrices, (in Russian)*, Sib. Math. Zhurnal **9** (1968), 152–164.

[39] Smith, L., *On the invariant theory of finite pseudoreflection groups*, Arch. Math. **44** (1985), 225–228.

[40] Stepanov, S. A., *Polynomial invariants of finite groups over fields of prime characteristic, (in Russian)*, Diskret. Mat. **11** (1999), 3–14.

[41] Vaccarino, F., *The ring of multisymmetric functions*, Ann. Inst. Fourier (Grenoble) **55** (2005), 717–731.

[42] Vaccarino, F., *Linear representations, symmetric products and the commuting scheme*, J. Algebra **317** (2007), 634–641.

[43] Weyl, H., "The classical groups", Princeton University Press, 1939.

M. Domokos
Rényi Institute of Mathematics,
Hungarian Academy of Sciences,
P.O. Box 127,
1364 Budapest, Hungary
domokos@renyi.hu